BS

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,999	03/04/2002	Anssi Tuomas Aura	MS183173.1/40062.181US01	6783

22801 7590 12/23/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
DOAN, PHUOC HUU	
ART UNIT	**PAPER NUMBER**
2687	6

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,999	AURA, ANSSI TUOMAS	
	Examiner	Art Unit	
	Phuoc H Doan	2687	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,11,12,15,16,18-34,37-44,48 and 49* is/are rejected.

7)☒ Claim(s) *9,10,13,14,17,35,36 and 45-47* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *05/10/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 11-15, 18-29, 31-32, 37-44, and 48-49 are rejected under 35 U.S.C. 102(e) as being anticipated by Holcman et al (US Pub. No: 2003/0108007).

As to claim 1, Holcman et al. disclose a computer program product encoding a computer program for executing a computer process on a mobile node (Fig. 3, col. 5, par. [0051]), a network being coupled to a first base station and a second base station and the mobile node being fully authenticated by the first base station for fully authenticated access to the network (col. 4, par. [0040-0041], and col. 5, par. [0056]), the computer process providing the mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node by the second base station (col. 6, par. [0063-0065]), the computer process comprising: receiving at the mobile node a credential from the first base station (col. 5, par. [0051-0052]), conditionally upon full authentication of the mobile node by the first base station (col. 5, par. [0052-0057]); transmitting from the mobile node an authentication message including the credential to the second base station to request

credential authentication from the second base station (col. 6, par. [0059-0066]); and receiving credential authenticated access to the network for the mobile node through the second base station (col. 6, par. [0064-0065]), if the second base station verifies the credential transmitted by the mobile node (col. 6 through col. 7, par. [0066-0070]).

As to claim 2, Holcman et al. further disclose that wherein the computer process further comprises: initiating a full authentication dialog with the second base station (col. 6, par. [0063-0065]); and completing the full authentication dialog with the second base station (col. 6, par. [0059-0062]), responsive to the operation of receiving credential authenticated access to the network (col. 6, par. [0063-0066]).

As to claim 3, Holcman et al. further disclose that wherein the credential is generated by the first base station (col. 4, par. [0040-0041]).

As to claim 4, Holcman et al. further disclose that wherein the computer process further comprises: receiving a challenge from the second base station (col. 5, par. [0054]); and computing the authentication message based on an element of the challenge (col. 5, par. [0055-0058]), wherein the operation of transmitting the authentication message is responsive to the operations of receiving the challenge and computing the authentication message (col. 6, par. [0063-0067]).

As to claim 11, Holcman et al. further disclose that wherein the credential includes at least one trust parameter (col. 7, par. [0069]).

As to claim 12, Holcman et al. further disclose that wherein the first and second base stations share a shared key and the computer process further comprises:

authenticating the credential by cryptographic computation based on the shared key and data included in the credential (col. 7, par. [0070-0071]).

As to claim 15, Holcman et al. further disclose that wherein the computer process further comprises: establishing a credential key with the first base station (col. 5, par. [0056]), responsive to full authentication of the mobile node through the first base station (col. 5, par. [0051-0052]), the credential key being associated with the credential (col. 6, par. [0065-0066]).

As to claim 18, Holcman et al. disclose that in a network coupled to a first base station and a second base station and the mobile node being fully authenticated by the first base station for fully authenticated access to the network (col. 4, par. [0040-0041], and col. 5, par. [0056]), a method for providing the mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node by the second base station (col. 6, par. [0063-0065]), the method comprising: receiving at the mobile node a credential from the first base station (col. 5, par. [0051-0052]), conditionally upon full authentication of the mobile node by the first base station (col. 5, par. [0052-0057]); transmitting from the mobile node an authentication message including the credential to the second base station to request credential authentication from the second base station (col. 6, par. [0059-0066]); and receiving credential authenticated access to the network for the mobile node through the second base station (col. 6, par. [0064-0065]), if the second base station verifies the credential transmitted by the mobile node (col. 6 through col. 7, par. [0066-0070]).

As to claim 19, Holcman et al. disclose a mobile node capable of coupling to a network (Fig. 1, col. 3, par. [0038-0039]), the network being coupled to a first base station and a second base station and the mobile node being fully authenticated by the first base station for fully authenticated access to the network (col. 4, par. [0040-0041], and col. 5, par. [0056]), the mobile node being capable of accessing with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node by the second base station (col. 6, par. [0063-0065]), the mobile node comprising: a reception module receiving at the mobile node a credential from the first base station (Fig. 3, col. 5, par. [0051-0052]), conditionally upon full authentication of the mobile node by the first base station (col. 5, par. [0052-0057]); and a transmission module transmitting from the mobile node an authentication message including the credential to the second base station to request credential authentication from the second base station (col. 6, par. [0059-0066]), wherein the reception module and the transmission module participate in credential authenticated access to the network for the mobile node through the second base station (col. 6, par. [0064-0065]), if the second base station verifies the credential transmitted by the mobile node (col. 6 through col. 7, par. [0066-0070]).

As to claim 20, Holcman et al. disclose a computer program product encoding a computer program for executing a computer process on a mobile node (Fig. 3, col. 5, par. [0051]), the computer process providing the mobile node with credential authenticated access to a network through a first base station after termination of fully authenticated access to the network through the first base station (col. 6, par. [0065-

0066]), the computer process comprising: receiving a credential from the first base station (col. 5, par. [0051-0052]), responsive to full authentication of the mobile node through the first base station (col. 4, par. [0040-0041], and col. 5, par. [0056]); detecting that fully authenticated access through the first base station has been terminated (col. 6, par. [0065-0066]); transmitting an authentication message including the credential to the first base station to request credential authentication from the first base station (col. 5, par. [0051-0052]); and receiving the credential authenticated access to the network through the first base station (col. 5, par. [0051-0052]), if the first base station verifies the credential transmitted by the mobile node (col. 6, par. [0059-0062]).

As to claim 21, Holcman et al. further disclose that wherein the computer process further comprises: initiating a full authentication dialog with the first base station (col. 4, par. [0040-0041]), responsive to the detecting operation (col. 5, par. [0052-0057]); and completing the full authentication dialog with the first base station, responsive to the operation of receiving the credential authenticated access to the network (col. 4, par. [0040-0041], and col. 5, par. [0056]).

As to claim 22, Holcman et al. disclose a method of providing a mobile node with credential authenticated access to a network through a first base station after termination of fully authenticated access to the network through the first base station (col. 5, par. [0051]), and col. 6, par. [0065-0066]), the method comprising: receiving a credential from the first base station (col. 5, par. [0051-0052]), responsive to full authentication of the mobile node through the first base station (col. 4, par. [0040-0041], and col. 5, par. [0056]); detecting that fully authenticated access through the first base

station has been terminated (col. 6, par. [0065-0066]); transmitting an authentication message including the credential to the first base station to request credential authentication from the first base station (col. 5, par. [0051-0052]); and receiving the credential authenticated access to the network through the first base station (col. 5, par. [0051-0052]), if the first base station verifies the credential transmitted by the mobile node (col. 6, par. [0059-0062]).

As to claim 23, Holcman et al. disclose a mobile node capable of establishing credential authenticated access to a network through a first base station after termination of fully authenticated access of the mobile node through the first base station (col. 6, par. [0065-0066]), the mobile node comprising: a reception module receiving a credential from the first base station (col. 5, par. [0051-0052]), responsive to full authentication of the mobile node through the first base station (col. 4, par. [0040-0041, and col. 5, par. [0056]); a detector module (Fig. 3, items 46, 48) detecting that fully authenticated access through the first base station has been terminated (col. 6, par. [0065-0066]); a transmission module transmitting an authentication message including the credential to the first base station to request credential authentication from the first base station (col. 5, par. [0051-0052]), wherein the reception module and the transmission module participate in the credential authenticated access to the network through the first base station (col. 5, par. [0051-0052]), if the first base station verifies the credential transmitted by the mobile node (col. 6, par. [0059-0062]).

As to claim 24, Holcman et al. disclose a computer program product encoding a computer program for executing a computer process on a computer system (Fig. 3, col. 5, par. [0051]), a network being coupled to a first and a second base station (col. 4, par. [0040-0041]), the computer process providing a mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node through the second base station (col. 6, par. [0063-0065]), the computer process comprising: receiving a request for full authentication from the mobile node (col. 5, par. [0051-0052]); fully authenticating the mobile node to provide fully authenticated access the network (col. 4, par. [0040-0041], and col. 5, par. [0056]); and transmitting a credential to the mobile node (col. 6, par. [0060]), the credential including at least one trust parameter to allow the second base station to grant credential authenticated access to the network by the mobile node prior to completion of full authentication of the mobile node by the second base station (col. 6, par. [0061-0067]).

As to claim 25, Holcman et al. further disclose that wherein the first and second base stations shared a shared key and the computer process further comprises: encrypting a credential key and at least one trust parameter using the shared key to generate the credential (col. 5, par. [0058], and col. 6, par. [0064-0065]).

As to claim 26, Holcman et al. further disclose that wherein the computer process further comprises: computing an authentication code for the credential key and the at least one trust parameter using the shared key (col. 6, par. [0064-0066], and col. 7, par. [0069]).

As to claim 27, Holcman et al. further disclose wherein the first and second base stations share a shared key and the computer process further comprises: encrypting a credential key, at least one trust parameter (col. 7, par. [0068-0069]), and a keyed one-way function result based on the shared key to generate the credential (col. 6, par. [0061-0062]), the keyed one-way function being a function of the credential key and the at least one trust parameter (col. 6, par. [0060-0066], and col. 7, par. [0068-0070]).

As to claim 28, Holcman et al. further disclose that wherein the first and second base stations share a shared key and the computer process further comprises: generating a credential key from a keyed one-way function based on the shared key, the keyed one-way function being a function of a nonce (col. 6, par. 0059-0067]).

As to claim 29, this claim is rejected for the same reason as set forth in claim 28.

As to claim 31, this claim is rejected for the same reason as set forth in claim 25.

As to claim 32, this claim is rejected for the same reason as set forth in claim 12.

As to claim 37, Holcman et al. disclose that in a network coupled to a first and a second base station (col. 4, par. [0040-0041]), a method of providing a mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node through the second base station (col. 6, par. [0063-0065]), the method comprising: receiving a request for full authentication from the mobile node (col. 5, par. [0051-0052]); fully authenticating the mobile node to provide fully authenticated access the network (col. 4, par. [0040-0041], and col. 5, par. [0056]); and transmitting a credential to the mobile node (col. 6, par. [0060]), the credential allowing the second base station to grant credential authenticated

access to the network by the mobile node prior to completion of full authentication of the mobile node by the second base station (col. 6, par. [0061-0067]).

As to claim 38, this claim is rejected for the same reason as set forth in claim 11.

As to claim 39, Holcman et al. disclose a first base station providing a mobile node with credential authenticated access to the network through the second base station prior to completion of full authentication of the mobile node through the second base station (col. 4, par. [0040-0041], and col. 5, par. [0056]), the first base station comprising: a reception module receiving a request for full authentication from the mobile node (col. 5, par. [0051-0052], and col. 6, par. [0065]); an authentication module fully authenticating the mobile node to provide fully authenticated access the network (col. 4, par. [0040-0041], and col. 5, par. [0056]); and a transmission module transmitting a credential to the mobile node (col. 6, par. [0060]), the credential allowing the second base station to grant credential authenticated access to the network by the mobile node prior to completion of full authentication of the mobile node by the second base station (col. 6, par. [0061-0067]).

As to claim 40, this claim is rejected for the same reason as set forth in claim 11.

As to claim 41, Holcman et al. disclose a computer program product encoding a computer program for executing a computer process on a computer system (Fig. 3, col. 5, par. [0051]), wherein the network is coupled to a first and a second base station and the mobile node is fully authenticated by the first base station (col. 4, par. [0040-0041], and col. 6, par. [0065-0066]), the computer process for providing a mobile node with credential authenticated access to a network through a second base station prior to full

authentication of the mobile node by the second base station (col. 6, par. [0063-0065]), the mobile node having a credential received from the first base station responsive to full authentication by the first base station (col. 4, par. [0040-0041], and col. 5, par. [0056]), the computer process comprising: transmitting a challenge (col. 5, par. [0054], and [0058]); receiving an authentication message from the mobile node (col. 5, par. [0051-0052]), responsive to the challenge (col. 5, par. [0054]), the authentication message including the credential to request credential authentication (col. 6, par. [0063-0066]); verifying the credential received from the mobile node (col. 6, par. [0065-0067]); and granting the mobile node with credential authenticated access to the network (col. 4, par. [0040-0041]), if the credential transmitted by the mobile node is verified (col. 6, par. [0059-0062]).

As to claim 42, Holcman et al. further disclose that wherein the computer process further comprises: receiving a request for full authentication from the mobile node (col. 5, par. [0051-0052]); granting the request for full authentication responsive to the operations of granting the mobile node with credential authentication access to the network and receiving a request for full authentication (col. 4, par. [0040-0041], and col. 5, par. [0056], and col. 6, par. [0060]).

As to claim 43, this claim is rejected for the same reason as set forth in claim 3.

As to claim 44, this claim is rejected for the same reason as set forth in claim 12.

As to claim 48, Holcman et al. disclose that in a network coupled to a first base station and a second base station (col. 4, par. [0040-0041]), a method of providing a mobile node with credential authenticated access to the network through the second

base station prior to full authentication of the mobile node by the second base station (col. 4, par. [0040-0041]), the mobile node having previously been fully authenticated by the first base station (col. 6, par. [0065-0066]), the mobile node having a credential received from the first base station responsive to full authentication by the first base station (col. 4, par. [0040-0041], and col. 5, par. [0056]), the method comprising: transmitting a challenge (col. 5, par. [0054], and [0058]); receiving an authentication message from the mobile node (col. 5, par. [0051-0052]), responsive to the challenge (col. 5, par. [0054]), the authentication message including the credential to request credential authentication (col. 6, par. [0063-0066]); verifying the credential received from the mobile node (col. 6, par. [0065-0067]); and granting the mobile node with credential authenticated access to the network (col. 4, par. [0040-0041]), if the credential transmitted by the mobile node is verified (col. 6, par. [0059-0062]).

As to claim 49, Holcman et al. disclose that an authenticating base station for providing a mobile node with credential authenticated access to a network through the authenticating base station prior to full authentication of the mobile node through the authenticating base station (col. 6, par. [0063-0066]), the mobile node having a credential received from another base station responsive to being fully authenticated by the other base station (col. 5, par. [0051-0057], and col. 7, par. [0068-0070]), the authenticating base station comprising: a transmission module transmitting a challenge (col. 5, par. [0054-0058]); a reception module receiving an authentication message from the mobile node (col. 5, par. [0051-0052]), responsive to the challenge (col. 5, par. [0054]), the authentication message including the credential to request credential

authentication (col. 6, par. [0063-0066]); and an authenticating module verifying the credential received from the mobile node and granting the mobile node with credential authenticated access to the network (col. 4, par. [0040-0041]), if the credential transmitted by the mobile node is verified (col. 6, par. [0059-0062]).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-8, 16,30, and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holcman et al. in view of Agrawal et al (US Patent No: 6,788,660).

As to claim 5, Holcman et al. disclose all the limitation of claim 1. However, Holcman et al. do not specific disclose that wherein the computer process further comprises: establishing a credential key cryptographically associated with the credential to prevent use of the credential without possession of the credential key.

Agrawal et al. disclose that wherein the computer process further comprises: establishing a credential key cryptographically associated with the credential to prevent use of the credential without possession of the credential key (col. 4, par. [44-67], and col. 21, lines 1-50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention to provide a credential key cryptographically of Agrawal et al. to the system of Holcman et al. in order to ensuring completion of the signaling

operation as a mobile terminal is handed off from one cell to another in prevent of the hacker.

As to claim 6, the combination of Holcman et al. and Agrawal et al. further disclose that wherein the credential key is a secret key and the operation of computing the authentication message comprises: computing a keyed one-way function based on the credential key and a challenge (col. 21, lines 25-40 of Agrawal et al.).

As to claim 7, this claim is rejected for the same reason as set forth in claim 5.

As to claim 8, this claim is rejected for the same reason as set forth in claim 5.

As to claim 16, this claim is rejected for the same reason as set forth in claim 6.

As to claim 30, this claim is rejected for the same reason as set forth in claim 6.

As to claim 33, this claim is rejected for the same reason as set forth in claim 6.

As to claim 34, this claim is rejected for the same reason as set forth in claim 6.

Allowable Subject Matter

Claims 9-10, 13-14, 17, 35-36, and 45-47 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As to claim 9, the prior art of record do not disclose the computer program product of claim 5 wherein the credential key is a public key of a public-key cryptosystem and the credential includes data for authenticating the credential key.

As to claim 10, the prior art of record do not disclose the computer program product of claim 1 wherein the computer process further comprises: determining a

challenge time from a synchronized clock set; and computing the authentication message based on the challenge time, wherein the operation of transmitting the authentication message is responsive to the operations of determining the challenge time and computing the authentication message.

As to claim 13, the prior of record do not disclose the computer program product of claim 12 wherein the credential contains a received result of a keyed one-way function, and the authentication operation comprises: computing a computed result of the keyed one-way function based on the shared key and the credential key; and comparing the computed result with the received result.

As to claim 17, the prior art of record do not disclose the computer program product of claim 15 wherein the operation of establishing the credential key comprising: sending a public key of a public key cryptosystem to a first base station via an authenticated communication link.

As to claim 35, the prior art of record do not disclose the computer program product of claim 33 wherein the credential key is a public key and the credential includes data for computing the credential key.

As to claim 36, the prior art do not disclose the computer program product of claim 33 wherein the credential key is a public key of a public-key cryptosystem and the credential includes data for authenticating the credential key.

As to claim 45, the prior art of record do not disclose the computer program product of claim 41 wherein the first and second base stations share a shared key, the challenge includes a challenge nonce, the authentication message includes a received

keyed one-way function result and an encrypted credential key, and the verifying operation comprises: decrypting the credential using the shared key; computing a computed result of the keyed one-way function using the credential key and the challenge nonce; and verifying the credential, if the computed result of the keyed one-way function matches the received keyed one-way function result.

As to claim 46, the prior art of record do not disclose the computer program product of claim 41 wherein the first and second base stations share a shared key, the challenge includes a challenge nonce, the authentication message includes at least one received trust parameter, a first received keyed one-way function result, a second received keyed one-way function result, a nonce of the first base station, and a credential key, and the verifying operation comprises: computing a computed credential key using the shared key and the nonce of the first base station; computing a first computed keyed one-way function result using the nonce of the first base station and the received trust parameters based on the shared key; and trusting the computed credential key, if the first computed keyed one-way function result matches the first received keyed one-way function result.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Uhlik et al. (US Pub. No: 2003/0028649) disclose "Method and apparatus for generating and identifier to facilitate deliver of enhanced data services in a mobile computing environment".

Mohammed (US Pub. No: 2003/0176186) discloses "Method for automatic and seamless call transfers between a licensed wireless system and an unlicensed wireless system".

Gallagher et al. (US Pub. No: 2004/0192211) disclose "Apparatus for supporting the handover of a telecommunication session between a licensed wireless system and an unlicensed wireless system".

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Phuoc H Doan whose telephone number is 703-305-6311. The examiner can normally be reached on 9:30 AM - 6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester G Kincaid can be reached on 703-308-7745. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Phuoc Doan

Art Unit: 2687

10/29/04
LESTER G. KINCAID
PRIMARY EXAMINER